AMERICAN UNIVERSITY
WASHINGTON, DC

University Policy: Information Technology Security Policy

Policy Category: Information Technology Policies

Subject: These security policies are provided to all members of the University community to establish requirements for each individual to follow in order to safeguard the University's academic and administrative information resources.

Responsible Executive: Vice President and Chief Information Officer

Office Responsible for Review of this Policy: Office of Finance and Treasurer and the Office of Information Technology (OIT)

Procedures: IT Security Guidelines, Network Host Security Standard (*access is limited to System Administrators. Please make requests through OIT Help Desk*).

Related University Policies: Data Breach Notification Policy, Data Classification Policy, Data Security for Mobile Devices, Electronic Mass Communication Policy, Records Retention and Disposal Policy, Responsible Use of University Technology Resources Policy

---

I. SCOPE

American University (AU) conducts significant portions of its operations via wired and wireless computer networks. The confidentiality, integrity and availability of the information systems, applications, and data stored and transmitted over these networks are critical to the University's reputation and success. AU systems and data face threats from a variety of ever-changing sources. AU is committed to protecting its systems and data from these threats, and therefore has adopted the following objectives to achieve a reasonable degree of information technology security:

- To enable all members of the University community to achieve their academic or administrative work objectives through use of a secure, efficient, and reliable technology environment.
- To protect academic, administrative, and personal information from current and future threats by safeguarding its confidentiality, integrity and availability.
- To establish appropriate policies and procedures to protect information resources from theft, abuse, misuse, or any form of significant damage while still enabling community members to fulfill their roles.
- To establish responsibility and accountability for information technology security within the organization.
- To encourage and support management, faculty, staff and students to maintain an appropriate level of awareness, knowledge and skill to enable them to minimize the occurrence and severity of information technology security incidents.
- To ensure the University is able to effectively respond to, contain, and address significant security incidents, while being able to continue its instructional, research, and administrative activities.

There is no interest on the part of the University to abridge academic freedom or personal speech rights, or to monitor or track personal behavior for reasons unrelated to technical operations or compliance with these policies. Automated procedures are used, wherever possible, to assess and process potentially relevant activity, thereby limiting the degree of individual staff involvement.

II. POLICY STATEMENT

Information and communication system resources are essential assets of AU. The entire community is responsible for ensuring that computing and communication facilities are used in an effective, efficient, ethical, and lawful manner.

While these policies identify many roles and responsibilities for safeguarding information resources; they cannot possibly cover every situation or future development. Therefore, this is to be considered a "living document" which will be modified or changed as needs require. It will be reviewed on at least an annual basis for corrections and to ensure compliance with current rules and regulations. You are encouraged to submit your suggestions for improvement to CIO@american.edu.

III. DEFINITIONS

Individuals: Access to the network requires an authorized relationship with the University, normally evidenced by the existence of current credentials within the enterprise directory. In addition, users must:

- Agree to abide by all applicable policies.
- Cooperate with the process of registering each device used for network access.
- Familiarize themselves with the operating procedures and unique requirements of the devices and software applications they use.

University Guests or Members of the Public: Individuals visiting the University - for example, parent or lecturer - or members of the public - for example, someone visiting AU in its role as a Federal Depository Library - may require temporary access to the AU network. A University member can facilitate the creation of a temporary "visitor account" to provide limited Internet access through the AU network. If general access to the internet is all that is required, University Guests may use the guest wireless network, which is not managed or monitored by AU.

Network-Attached Devices: In order for a device to communicate with the Internet or other devices attached to the AU network, it must first be associated with an authorized individual.

Confidential and Regulated Data Information: Please see the University's Data Classification Policy for a complete description of confidential data and guidance on how to safeguard AU data for each classification.

IV. POLICY

A. APPLICABILITY

These policies apply to all members of the University community, including students, faculty, staff, vendors, volunteers, contractors, consultants and any other person having access to AU institutional information or technology resources.

These policies apply to all electronic information system resources of AU, including technology hardware and software owned, leased, or licensed by AU. This includes hardware and software used to process,

store, retrieve, and display and transmit electronic representations of data, voice, and video content.

Personally, owned equipment is also covered if it is used to process AU institutional information or if it is connected, directly or indirectly, to the AU network. The University will not access or modify software or information stored on personally owned equipment without permission of the owner; however, access to the AU network may be denied or limited unless these policies are complied with fully.

B. SECURITY ROLES AND RESPONSIBILITIES

Information technology security is the responsibility of all students, faculty, and staff. Every person handling information or using University information resources is expected to observe these information technology security policies and procedures, both during and, where appropriate, after their time at the University.

Development of these policies is the responsibility of the Chief Information Security Officer. Implementation is managed by OIT, in some cases with the assistance of designated personnel with security responsibilities in other areas of the University, and with appropriate legal review. University senior management, the Office of General Counsel, and the Office of Risk Management may provide advice for new security issues.

OIT will assist all members of the University community to facilitate compliance with these policies through the publication of information technology security alerts, guidelines, technical documentation, required security training, and support for an ongoing information technology security awareness program.

Since OIT cannot be directly responsible for all campus technology resources, users throughout the community share in the task of maintaining information technology security. In larger or more complex departments, there may be one or more employees assigned to provide departmental personal computer support. It is expected that these technical support administrators will employ OIT recommended practices and procedures, and cooperate with OIT in addressing security problems.

Although OIT controls access to the AU network and application systems, individual end users control access to their personal computers and the files and applications installed on them. Therefore, the user of an individual computer is responsible for determining who has access to locally stored data and applications and for managing the appropriate level(s) of access.

C. STANDARDS

AU's technology environment is a shared and limited community resource subject to both malicious and unintended abuse. Computing systems and other specialized devices have the potential to introduce security risks, especially when they are attached to a communications network. To mitigate risk, standards for managing and securing applications, workstations, servers, network devices, and third-party services have been developed.

As new equipment or applications are introduced into the environment, a risk assessment should be conducted to ensure compliance with these standards prior to use or connecting to the AU network. OIT staff and the University's internal and external auditors will periodically conduct compliance reviews and test for vulnerabilities in University-owned systems and networks to ensure that systems and applications are updated as new vulnerabilities are discovered and threats revealed.

D. REQUIREMENTS

General Requirements:

1. **Network User Names, Passwords and Multi-factor Authentication**

   Logical access controls can prevent or discourage unauthorized access to information resources and help ensure individual accountability. Therefore, individual users must be identified and granted appropriate levels of access to network devices by means of a unique User Name coupled with a password and/or some other form of secure authentication process, such as multifactor authentication. A unique User Name is required to provide for individual accountability in audit logs, etc. For this reason, generic or group IDs are not permitted.

   Default manufacturer passwords must be changed. All enterprise passwords must be composed in accordance with the following naming conventions:

   16character passwords must:

   - Change every 365 days
   - Begin with an alphabetic character.
   - Contain at least one lowercase letter and one uppercase letter.
   - Not have been used for your last 2 passwords (at least two digits should change).

2. **Secure Verification of User Name and Password**

   Under some conditions, it is possible to eavesdrop on network traffic. For this reason, all authentication procedures must use a current encryption mechanism. This means that only versions of popular e-mail, file transfer, and other network access programs that support encrypted authentication methods may be used.

3. **Third-Party Services**

   When a third-party is used to provide services or to store data, security requirements should be considered and made part of any contractual agreements. Such vendor agreements must include appropriate safeguards for the security of the University's information and resources and audit rights. Consult with the Director of Contracts and Procurement to ensure that contract/agreement language is appropriate. See IT Security Guidelines for additional information. Vendors and independent contractors (hereinafter collectively "Vendors") may only have access to the minimum necessary information to perform the tasks for which they have been retained. Vendors must comply with all applicable AU policies and practices. Vendor access must be uniquely identifiable. Major vendor work activities should be logged and include such events as personnel changes, password changes, milestones reached, deliverables, and arrival and departure times.

   Upon departure of a vendor employee, the vendor must be required to inform AU, so that the vendor employee access may be terminated and return or destroy all sensitive information, and surrender all AU identification badges, access cards, equipment and supplies immediately.

Hardware (all network connected devices) Requirements:

1. **Device Authentication**

   Each device will be prompted to authenticate, using the credentials of the University community member operating that device before gaining access to the University's wired or wireless network. An exception is the Guest network which is provided and supported via a third-party contract. American University business should not be conducted on the Guest wireless network.

2. **Equipment Disposal**

   Confidential University academic or administrative information is likely to be present on storage media associated with obsolete or surplus equipment intended for disposal and must be disposed of by the University's asset management contractor. Disposal guidelines can be found in the University's Records Retention and Disposal Policy.

3. **Server Registration**

   If a network device provides services to multiple users, whether the services are restricted to on campus or publicly accessible, there are additional registration requirements, as allowing other systems to initiate connections increases the University's risk to threats. Outside systems cannot successfully achieve such connections unless the University system is publicly addressable, i.e. unless it has a Public Internet Address. Registration information will include the name and contact information for the person who is responsible for administering the system and verification by OIT that appropriate security configurations are in place. The registrant must describe any confidential data, stored on the system; as such data is defined in the University's Data Classification Policy and details about the configuration. Contact the OIT Help Desk to register servers.

   Registrants are responsible for notifying the OIT if the profile of the system changes. Additionally, OIT will send out, at a minimum, an annual request for update of information about known registered systems.

4. **Assignment of Network Identifiers**

   In order to ensure reliable network operation, all devices must be configured to accept the assigned Internet Protocol (IP) numeric address, AU-generated identifying name, and other network parameter s which are automatically assigned each time a network connection is established. The use of permanent network identifiers is restricted to OIT-managed or approved devices.

5. **Security Configuration**

   Departments and administrative units are responsible for ensuring the security and safety of departmental network devices that provide services to multiple users. They will develop and administer their own local procedures for timely patching of systems, establishing secure configurations, and ensuring that the Network and Host Security Standard referenced in this policy are met. OIT will monitor the network to verify that appropriate security configurations are met.

Software Requirements:

1. **Anti-Virus Software**

Computers infected with viruses or malicious code can jeopardize information technology security by contaminating, damaging, and destroying data. Therefore, current anti-virus software must be installed and operating with the most current list of virus definitions. The University has licensed anti-virus software for use by every AU student, faculty, or staff member using the network.

2. Firewall Software

All users must enable firewall software on their computers to restrict all but what is required for business use.

3. Licensed Software

Software installed on any AU computer system must be legally licensed. Audits may be conducted at any time to ensure this objective. AU department heads are responsible for ensuring that no software license usage in their department exceeds purchased levels and arranging for additional licensed copies when needed to support instructional or administrative activities.

4. Software Patch Updates

All currently available security patches for operating systems and application software must be installed. Software which is "end of life" and/or for which security patches are not routinely made available should not be used on the AU network.

5. Secure Data Transmission

When employees are working at an off-campus location and remotely connecting to systems on the AU network, an encrypted communication channel must be used in order to protect the confidentiality of User Names, passwords, and University records containing personal, confidential, or legally protected information.

A general-purpose encrypted communication link can be accomplished through use of "virtual private network" (VPN) technology. By accessing the AU network via this client, the security requirements of this section will be met. When using AU's VPN technology with personal equipment, users must understand that their machines are acting as an extension of AU's network, and as such are subject to the same rules and regulations that apply to AU-owned equipment.

6. Secure Data Storage

Sensitive personal information must be stored within University systems using an approved method of encryption to help secure the data in the event of unauthorized access. This requirement is especially important when information is stored on portable devices, including mobile devices. See Data Security for Mobile Devices Policy.

E. PROHIBITED PRACTICES

1. General Activities

Users may not engage in any unlawful activity or transmit material in violation of applicable local, state or federal laws, University policy, or industry regulations. Users must not purposely engage in activity that may harass, threaten or abuse others; degrade the performance of information resources; deprive an authorized user of access to a technology

resource; or attempt to circumvent AU's security measures.

Users must not attempt to access data or programs contained on University systems for which they do not have authorization. Users may not share account(s), passwords, security tokens, or similar information or devices used for identification and authorization purposes.

Users must not take any action that violates the University's codes of conduct, academic integrity policy, Staff Personnel Policies Manual, Faculty Manual, information technology security policies or other applicable laws. In the event of a conflict between policies, the more restrictive policy shall govern.

2. Commercial Use

AU technology resources may not be used for solicitations, commercial purposes, or any business activities for individuals, groups, or organizations without prior permission obtained from the Provost or Vice President and Treasurer. Note that this policy does not apply to the promotion of scholarly works by faculty members.

3. Copyright and Illegal Software and Materials

Users are prohibited from making, distributing, or using illegal copies of copyrightedmaterials or software. This includes illegally downloading software and materials from the Internet. No illegal copies of such materials or software may be stored on University systems,or transmitted over University networks. Users may not copy software applications from onecomputer to another unless legally permitted. Please refer to the University's Responsible Use of University Technology Resources Policy.

4. Email

The following activities are prohibited because they impact the performance of the mail systems and may expose sensitive data to unauthorized access:

- Intentionally sending or forwarding e-mail containing malicious software, links or attachments.
- Sending, forwarding or receiving confidential or sensitive academic or administrative information through non-AU e-mail accounts.
- Confidential AU information must not be stored in or transmitted through email.
- Sending unsolicited messages to large groups except when necessary to fulfill the academic or administrative mission of the University.
- Sending excessively large (for example, over 30 million characters) or numerous (for example, over 1,000) messages except when coordinated in advance with OIT.
- Sending or forwarding chain letters.

5. Network Monitoring

Users may not conduct network scans searching for other connected devices or conduct any form of network monitoring that will intercept data not intended for the user's computer. Unless this activity is a part of an authorized employee's normal job duty, users must not download, install or run programs designed to reveal or exploit weaknesses in system security such as password discovery programs, packet sniffers, or port scanners.

6. Server and Network Operations

Unless specific authorization is received from OIT, individual users or departments must not

operate DHCP, DNS, proxy, e-mail, remote access, or connection sharing servers. Users may not implement individual or department servers for anything other than academic purposes. Users must not use external DNS providers to advertise services at AU network addresses. Users or departments must not install individual network components such as switches, routers, or wireless access points, or tamper with any network wiring.

7. Wireless Communication

Installation, engineering, maintenance, and operation of wired and wireless networks serving University faculty, staff, or students on any property owned or tenanted by the University are the sole responsibility of OIT. Individuals and departments may not independently deploy wireless networking products without the approval of OIT.

F. ENFORCEMENT

Violations of this policy must be reported to the CIO who will investigate the incident and take appropriate remedial actions. Remedial actions could include, without limitation, the following:

- Temporary or permanent loss of access privileges.
- University sanctions as prescribed by student, faculty, or staff behavioral codes, including dismissal or termination from the University.
- Remedial education.
- Monetary reimbursement to the University or oilier appropriate sources.
- Prosecution under applicable civil or criminal laws (violations of local, state and federal law may be referred to the appropriate authorities).

The University may take any action that is necessary to investigate and address violations of these policies, including temporarily or permanently terminating network access or computer use privileges pending the outcome of an investigation or a finding that this policy has been violated.

In order to ensure compliance with these policies, OIT may:

- Monitor network traffic for the detection of unauthorized activity and intrusion attempts.
- View or scan any file or software stored on University systems or transmitted over University networks.
- Carry out and review the results of automated network-based security scans of systems and devices on the University network in order to detect known vulnerabilities or compromised hosts.
- Report recurring vulnerabilities over multiple scans to the departmental head or other appropriate manager.
- Take steps to disable network access to affected systems or devices if identified security vulnerabilities deemed to be a significant risk to others have been reported.
- Act unilaterally to contain the problem, up to and including isolating systems or devices from the network (every effort will be made to seek the cooperation of the user or appropriate contact for the system involved).
- Coordinate investigations into any alleged computer or network security compromises or security incident.
- Cooperate in the identification and prosecution of activities contrary to University policies or legal requirements. Actions will be taken in accordance with relevant University policies, codes and procedures with, as appropriate, the involvement of the general counsel's office, campus police, and law enforcement agencies.

Violations, complaints, or questions about this policy should be directed to CIO@american.edu.

G. ACCESS TO UNIVERSITY RECORDS

The University provides limited access to academic and administrative data to those whose educational or administrative responsibilities require it to perform their job function. Multiple levels of access exist which are generally determined by the nature of the position held rather than by the individual. This practice helps to ensure that data access restrictions are consistent and based on legal, ethical, and practical considerations. The University expects all custodians of its academic and administrative records to access and utilize this information in a manner consistent with the University's need for security, integrity, and confidentiality. Each University functional unit must develop and maintain clear and consistent procedures for access to academic and administrative data within its area of responsibility, and review access levels and procedures regularly. Note that nothing in these policies precludes or addresses the release of institutional data to external organizations or governmental agencies as required by legislation, regulation, or another legal vehicle.

1. Access Rights and Responsibilities

Access rights for certain applications are automatically assigned based on role. Others, such as those for the Colleague system require intervention by OIT to maintain proper security. To request access rights for these systems, submit the access request form found at https://www.american.edu/oit/accounts/Account-Request.cfm. OIT will confirm approval of the request with the appropriate department manager or other University data custodian. Department managers must ensure that their representatives maintain only those access privileges required to perform their official job functions.

Users may only access, change, or delete data as required in fulfillment of assigned University duties. The following examples of prohibited behaviors are illustrative, not exhaustive:

- Do not change data about yourself or others for reasons other than usual administrative purposes.
- Do not use information (even if authorized to access it) to support actions by which individuals might profit (e.g., a change in salary, title, or band level; a better grade in a course, financial aid, parking permits, student account).
- Do not disclose information about individuals without prior supervisor authorization.
- Do not engage in any type of unauthorized data analyses (e.g., tracking a pattern of salary raises; determining the source and / or destination of telephone calls or Internet protocol addresses; exploring race and ethnicity indicators; looking up grades).
- Do not circumvent the nature or level of data access given to others by providing access or data sets that are broader than those available to them via their own approved levels of access (e.g., providing a University-wide data set of human resource information to a co-worker who only has approved access to a single human resource department).
- Do not facilitate another's illegal access to AU's administrative systems or compromise the integrity of the systems or data by sharing your passwords or other information.
- Do not violate University policies or federal, state, or local laws in accessing, manipulating, or disclosing University administrative data.
- Do not release institutional data to internal departments, external organizations or governmental agencies without prior approval of your supervisor.
- Do not copy for personal use any University document unless authorized.
- Do not retrieve, view, or examine any University document or file, except those to which

you are given access or otherwise authorized to handle.

Enforcement of these guidelines will be pursued as outlined in Section F of this document.

2. Privacy

All files created or maintained on University-owned computers or stored within University-owned systems are subject to University privacy policies. While access to files is limited to those intended to have it, authorized University officials can examine the contents of all files and operational logs maintained on University-owned equipment. Although every effort is made to respect the privacy and confidentiality of users' files, the University reserves the right to view or scan any file or software stored on University systems or transmitted over University networks. This will be done periodically to verify that software and hardware are working correctly, to preserve data for backup purposes, to look for disruptive forms of data or software such as computer viruses, to audit the use of University resources, and to ensure compliance with the law and with University policies.

All files are further subject to external review and possible public release resulting from a search warrant or subpoena issued and served pursuant to law. Disclosure of information from system logs or other usage records to officers of the law or to support internal disciplinary proceedings is only permitted when required by and consistent with the law, or when there is reason to believe that a violation of law or of a University policy has taken place. All external requests for information from system logs or other usage records must be submitted to the Office of General Counsel for review.

H. REPORTING A SECURITY BREACH

Because specific processes have been established to address security breaches, any suspected security breach should be reported immediately to the VP and Chief Information Officer, CIO@american.edu.

I. DATA BACKUP AND RECOVERY

Production servers and computers offering shared network resources are backed up regularly to provide protection against hardware failures and other disasters.

Individual computers are not backed up by OIT. It strongly recommends that users make individual backups of critical data.

A formal business continuity plan for technology resources is maintained by OIT.

J. SECURITY AWARENESS AND TRAINING

It is essential that all aspects of information technology security, including confidentiality, privacy and procedures relating to system access, be incorporated into formal student, faculty and staff orientation procedures and conveyed to existing University community members on a regular basis.

Required training is added to all full-time staff and faculty learning plans in AsuccessfulU and must be completed within 6 months of hire and annually thereafter.

OIT routinely holds meetings with departmental technical partners at which current and pending security issues and new potential risks are discussed and mitigation strategies are shared. OIT also hosts web pages containing resources on information and system security, knowledge base articles available at

Justask.american.edu and periodically posts tips via social media and the university newsletter.

Managers should review, at least annually or upon job description change, the duties of personnel under their supervision to determine if the position is one of special trust. Personnel whose duties bring them into contact with confidential or sensitive information should be required to provide written assurance of their intention to comply with the University security policies, attend an awareness training program at least annually, and receive periodic security briefings as necessary. Contact OIT HelpDesk and ask for a security briefing.

V. EFFECTIVE DATE AND REVISIONS:

This policy was effective June 19, 2006;
The policy revised November, 2010.
The policy was revised February 2013.
The policy was reviewed September 2015.
The policy was revised January 2016.
The policy was revised March 29, 2019.
The policy was revised September 10, 2021.